別紙 1

論文の内容の要旨

論文題目	Private Permutations in Card-based Cryptography （和訳：秘匿置換を用いたカードベース暗号に関する研究）
学位 申請者	中井　雄士

マルチパーティ計算(MPC) は，複数の参加者がそれぞれ持つ情報を秘匿したまま，参加者同士で協調してそれらの情報を入力値とした関数の計算を行う暗号プロトコルである．一般的なMPC は，計算機への実装が想定されている代数的なプロトコル（以下，代数的MPC）であるが，計算機を用いずに物理的な道具を用いて構成されるMPC も存在する．その中で，本研究ではトランプのような物理的なカードを用いてMPCを実現するカードベース暗号を扱う．

カードベース暗号は，カードを並べ替える，裏返すといった一般のカードゲームで用いられる操作によってMPCを実現する．このとき，従来のカードベース暗号は，すべての操作をテーブル上などの公開の場で行うことを仮定するパブリックモデルを採用していた．このモデルのもとでは，プレイヤの入力値を秘匿して表現する方法が，裏面のカードを用いる方法に限定される．その結果，1-bitの表現に最低でも2枚のカードが必要であり，n-bit入力のプロトコルの構成には最低でも$2n$ 枚のカードが必要であった．

また，パブリックモデルはランダム化も公開の場で行うことを要求するため，従来のカードベース暗号はシャッフルという物理的な仮定に基づいたランダム化を用いることでプロトコルの秘匿性を実現していた．しかし，「操作の結果は操作を行った本人も含め誰にも分からない」ことを要求するシャッフルは，代数的MPCで通常採用される内部乱数モデル（各プレイヤが内部でプライベートに乱数を生成・使用できる）とは相容れないものである．

本論文では，代数的MPCの内部乱数モデルと類似する新たなカードベース暗号の操作モデル「プライベートモデル」を提案する．プライベートモデルでは，プレイヤがローカルにカードを置換する操作「秘匿置換」を許す．また，このモデルでは，秘匿置換を用いた入力が可能となるため，入力に2枚のカードを用いる必要がない．その結果，パブリックモデルにおけるカード枚数の下限値を下回る枚数でプロトコルを構成できることをいくつかの例で示す．具体的には，論理演算，しきい値関数，大小比較に対するプロトコルの提案を行う．

本稿は全6章で構成される．第1章はMPCとカードベース暗号の背景説明である．第2章は，プライベートモデルの提案および記法の定義などの準備である．第6章は本論文のまとめである．3章から5章では，秘匿置換を用いて構成したプロトコルの提案を行う．具体的な内容は以下の通りである．

第3章：論理演算プロトコルの提案

本研究で提案するプライベートモデルでは，秘匿置換を入力に用いることが可能である．その結果，入力値をカード2枚で表現しなければならない制約がなくなり，従来のカード枚数の下限値を下回るプロトコルを構築することが可能となった．本章では，従来のパブリックモデルでは最低4枚必要な，2入力の論理演算プロトコルANDとORが，秘匿置換を導入した提案モデルにおいては3枚のカードで実現（計算）可能であることを示す．また，XORについては，2枚のカードで実現可能であることを示す．

第4章： 多数決およびしきい値関数プロトコルの提案

第3章で示したAND，OR プロトコルは，秘匿置換を用いて入力値表現を工夫することで，使用カード4枚で，ANDとORの結果を同時に得る2入力2出力のプロトコルへ拡張することができる．第4章では，このAND/OR同時計算プロトコルが，カードを追加することなく3入力多数決プロトコルへ応用できることを示す．さらに，この3入力多数決プロトコルを拡張することで，これまで$2n+2$ 枚のカードが必要であったしきい値関数プロトコルを$n+2$枚で実現できることを示す（nは入力数）．プライベートモデルではn入力のプロトコルには最低でも$2n$枚のカードが必要であるため，提案のしきい値関数プロトコルはその下限値のほぼ半分の枚数で実現できている．ここでも3章と同様に，入力値をカードで表現するのではなく，秘匿置換で表現したことが効率化の決め手となっている．また，手順数として評価する秘匿置換および通信回数に関しても，それぞれ$4n^2$をnへ，$2n^2$を$n-1$へ削減することができる．この結果から，秘匿置換は論理演算のような基礎プロトコルのみでなく，より高度な関数を計算するプロトコルに対しても効率化が達成できることがわかる．

第5章： 効率的なカードベース金持ち比べプロトコルの提案

内部乱数より自然に導入される秘匿置換をカードベース暗号に導入したことにより，カードベース暗号は代数的MPC により近いモデルとなった．それにより，独立的に研究が進められてきたカードベース暗号と代数的MPC間で相互にテクニックを活用できるようになることが期待される．本章では実際に，代数的MPCプロトコルである2つのm-bit値の大小比較（金持ち比べ）プロトコルをカードプロトコルに変換して，新たなプロトコルを構築する．変換はYaoのプロトコルの本質を用いればほぼ自明なものであり，オリジナルのプロトコルを非常に単純化している．Yaoの金持ち比べから得た提案プロトコルは，秘匿置換および通信回数では効率化に成功している一方で，カード枚数が指数的に増えてしまう課題があった．そこで本章では，ビット毎の大小比較に基づく，新しい大小比較プロトコルを提案する．提案プロトコルは，有名な論理パズル“The fork in the road”を用いる点でも興味深い．最終的に，金持ち比べプロトコルをたった6枚のカードで実現できることを明らかにした．また，秘匿置換および通信回数に関しても，それぞれ$12m-10$ を$2m+1$へ，$6m-5$を$2m$ へ削減する．これは秘匿置換の有効性を示す最も強力な例となっている．

別紙２

論文審査の結果の要旨

学位申請者氏名　　中井雄士

審査委員主査　　岩本　貢

委員　　吉浦　裕

委員　　﨑山一男

委員　　菅原　健

委員　　太田和夫

（*自筆署名の場合に限り、押印省略可）

マルチパーティ計算(Multi-Party Computation, MPC)は複数の参加者で入力を秘匿したまま，それらの関数値を協調計算する暗号プロトコルである．本研究では，トランプのような物理的なカードを用いてMPCを実現する手法（カードベース暗号プロトコル）の新しいモデルを提案し，従来モデルに対する有効性を示している．

カードベース暗号では，例えば，カードを裏返すことで暗号化を行い，相手に手渡すといったことが出来る．カードベース暗号において重要なのは，暗号化に用いられる，入力メッセージのランダム化（ランダム置換）である．従来のモデルでは，ランダム化は公開で行われ，ランダム化された結果，すなわちどの置換を選択したかは操作を行っている本人にすら分からないという仮定をおく．これは物理的にはカードを切り混ぜる（シャッフルとよぶ）ことで実現される．このようなモデルをパブリックモデルと呼ぶ．

通常の代数的なMPCでは，このようなパブリックモデルは実現出来ない．ランダム化に用いる乱数をプレーヤが発生させている以上，この乱数を他のプレーヤに秘匿することはできても，プレーヤ自身は知っていると考えざるを得ないためである．このように，プレーヤが発生させた乱数を公開せずに保持することで秘匿性を保証するモデルを，プライベートモデルと呼ぶ．本研究では，カードベース暗号におけるプライベートモデルを提案し，その有効性を考察している．

カードベースにおけるプライベートモデルを考えるために，本論文ではカードを公開でなくプライベートな場所（例えば，プレーヤが背中に隠すなど）でランダム化することを許す．パブリックモデルにおけるシャッフルに対する，プラーベートモデルでのこのようなランダム置換を，プライベート置換(Private Permutation, PP)とよぶ．パブリックモデルにおけるシャッフル操作は，近年数学的に複雑になっており，カードだけでは物理的に実現出来ないようなものも幾つか提案されているが，PPを用いれば，さまざまなランダム置換を実現出来る．ただし，悪意のある攻撃を考える必要のないパブリックモデルに対して，プライベートモデルではsemi-honest安全性を仮定しなければならないことに注意する．

パブリックモデルにおけるカードベース暗号では，入力を裏返したカードで表現するしかないため，1-bitの入力に2枚のカードが必ず必要となる．つまり，n-bit入力に対して$2n$枚のカードが最低限必要になる．一方でプライベートモデルでは，プライベートに入力を生成しても良いため，1-bitの入力に2枚のカードは必ずしも必要ない．例えば，背面でカードを置換することでカードを用いずに1-bit入力を表現するなどが可能である．本研究では，パブリックモデルにおけるカード枚数の下限を下回る枚数でプロトコルを構成できることをいくつかの例で示している．具体的には，論理演算，しきい値関数，大小比較に対するプロトコルの提案を行っている．

各章の具体的な成果（第3章から第5章）は以下の通りである．

第3章：プライベートモデルにおける，基本論理ゲートAND，OR，XORの実現手法を提案した．これらの論理ゲートは1-bit 2入力であるため，パブリックモデルでは最低4枚カードが必要である．PPを用いたプライベートモデルでは，ANDとORが3枚のカードで実現（計算）可能であり，XORについては2枚のカードで実現可能であることを示している．

第4章：3章で提案したAND/ORプロトコルの対称性を利用することで，AND/OR同時計算プロトコルを3枚のカードで実現出来ることを示した．これを応用すると，カードを追加することなく3入力多数決プロトコルを構成できる．さらにこれを拡張することで，しきい値関数プロトコルを$n+2$枚で実現できることを示している（n は入力数）．パブリックモデルにおける多数決プロトコルでは，これまで$2n+2$ 枚のカードが必要なものが知られており，カード枚数は約半分になることが分かる．また，手順数として評価する秘匿置換および通信回数に関しても，それぞれ$4n^2$をn へ，$2n^2$を$n-1$へ削減している．

第5章：パブリックモデルとプライベートモデルでは，ランダム化に関する仮定が全く異なるため，従来の代数的MPCとカードベース暗号の研究は独立に進んできた．本研究ではプライベートモデルにおけるカードベース暗号を考えるので，代数的なMPCの考え方をそのまま利用出来る場合がある．例えば，Yaoが提案した2つのm-bit値の大小比較（金持ち比べ）プロトコルはカードプロトコルに容易に変換できる．

しかし，このプロトコルは，秘匿置換および通信回数では効率化に成功している一方で，カード枚数が指数的に増えてしまう．そこでビット毎の大小比較に基づく，全く新しい大小比較プロトコルを提案している．提案プロトコルは，有名な論理パズル“The fork in the road”を用いる点でも興味深い．最終的には，このプロトコルに用いられるカードを再利用出来るように工夫することで，金持ち比べプロトコルはたった6枚のカードで実現できる．また，秘匿置換および通信回数に関しても，それぞれ$12m-10$ を$2m+1$へ，$6m-5$を$2m$ へ削減する．これは秘匿置換の有効性を示す最も強力な例となっている．

以上のように，本論文はカードベース暗号におけるプライベートモデルを新たに提案し，パブリックモデルにおけるカード枚数の下限を破るプロトコルを提案することで，提案モデルの有効性を示した．これまではシャッフルをベースとしたパブリックモデルの議論が中心であったカードベース暗号に，新しい研究の方向性とその可能性を示した論文ということが出来る．よって本論文は，博士（工学）の学位請求論文として十分な価値を有するものと認める．